Approved by the Committee on 14 November 2022

Information Governance Committee
Monday 29 August 2022 at 10am
MS Teams meeting

Present: Mrs Jean Ford, Non-Executive Board Member (Chair)
Mr Michael Breen, Non-Executive Board Member
Ms Sheila Cowan, Non-Executive Board Member
Mr Marc Mazzucco, Non-Executive Board Member
Cllr Douglas Reid, Non-Executive Board Member

Ex-officio: Mrs Lesley Bowie, Board Chair
Mr Derek Lindsay, Director of Finance and Senior Information Risk Owner
Ms Ann Wilson, Head of Information Governance (IG) and Data Protection Officer (DPO)

In attendance: Mr Hugh Currie, Assistant Director, Occupational Health, Safety and Risk Management
Mr Derek Gemmell, Acting Assistant Director, Digital Services
Ms Natali Higgins, Information Governance Manager (Corporate Records)
Mrs Angela O'Mahony, Committee Secretary (minutes)

1. Welcome / Apologies for absence

1.1 The Committee Chair welcomed Cllr Douglas Reid, Non-Executive Board Member, who had recently joined the Committee and Ms Ann Wilson, who had recently been appointed as the Head of Information Governance and Data Protection Officer, as well as invited guests.

1.2 Apologies were noted from Ms Claire Burden, Mr Robert Bryden, Ms Nicola Graham, Dr Crawford McGuffie and Ms Tara Palmer.

2. Declaration of any Conflicts of Interest

2.1 There were no conflicts of interest declared.

3. Draft Minute of the Meeting held on 9 May 2022

3.1 The minute of the meeting held on 9 May 2022 was approved as an accurate record of the discussion.

4. Matters Arising

4.1 The action log had previously been circulated to Committee members and all progress against actions was noted.

4.2 **IGC Work Plan 2022-2023** - The Committee noted the work plan.

5. Information Governance

5.1 **Digital/Cyber Security Network and Information Systems (NIS) Audit update**

The Acting Assistant Director, Digital Services, Mr Derek Gemmell, outlined the background to the three year audit and review programme to evaluate Scottish Health Boards' compliance with NIS regulations. Following the initial audit in 2022, NHSAA had recently completed the second annual review, with the procedure followed as detailed in the report. A report is expected later in the year to outline performance across all Board areas.

Committee members received a summary of the key results from the Review Report 2022. NHSAA had made significant progress over the last 12 months and compliance had risen from 54% to 73% during this period. There had been improvements in 15 of the 17 categories, with 13 categories at compliance level of 60 or more. The Board's overall compliance status had moved from amber to yellow, which indicated there was a minor risk of exposure but controls and procedures were working effectively. However, there was still further work to be done to improve compliance, in particular for four out of 76 categories in which the Board did not meet the required minimum compliance.

Mr Gemmell highlighted the activity taking place to further progress improvements in supplier management, including review of local and national contract templates for suppliers of third party services focusing on cyber security. Work was taking place to raise staff awareness at all levels of the organisation in relation to cyber security. In addition, work was ongoing related to incident management and business continuity. The auditor had particularly noted improvements related to supplier management and risk management. The Digital Champion network had been highlighted as an example of good practice.

Mr Gemmell confirmed in response to a question from a Committee member that there will be a review of the Cyber Security risk on the strategic risk register to reflect the work taking place to mitigate the risk, including the level of risk tolerance.

Mr Gemmell advised in response to a question from a Committee member that good progress had been made since the introduction of Microsoft 365 (M365) due to the high level of security inherent within these products. The Board was adopting a robust approach in relation to system patching.

Committee members noted the auditor's risk assessment and it was felt that the low risk related to Cyber Security did not reflect the cyber security risks currently being faced by the Board and other public sector organisations. Mr Gemmell explained that this was the auditor's assessment relative to controls assessed as part of the audit, as opposed to the wider risk faced which remains a key priority for the Board. Digital Services were working closely with Information Governance (IG) colleagues to mitigate the very high risk of cyber attack.

Mr Gemmell advised in response to a question from a Committee member that he would clarify with the auditors the RAG status of some actions marked as green but not achieved to understand their interpretation of progress made. Mr Gemmell would also clarify governance and reporting arrangements to monitor progress against outstanding actions. **DG**

Mr Gemmell advised in response to a question from a member that following the power outage at University Hospital Crosshouse in March 2022, a post-incident review had been carried out by a third party CGI. The outcome of the review had been included in a Significant Adverse Event Review report which had identified a number of recommendations to be taken forward through Risk Management, Resilience and Digital Services.

Committee members commended the progress being made and areas of good practice identified although it was recognised that there was still further work to be done. The Committee thanked the team involved for the work done to date.

Outcome: Committee members noted the summary of the 2022 NIS Audit Review Report and the progress made towards improving the status of the organisation's overall compliance with the NIS Regulations.

5.2 **Health Records update**

The Committee received an update on activities performed within Health Records Services that were within the remit of the Information Governance Committee.

The Committee Chair, Mrs Jean Ford, advised that she had some questions on the report which she would discuss with Mr Bryden out-with the meeting and ask him to report back to the next Committee meeting. **JF**

Outcome: Committee members noted the Health Records update.

5.3 **Public Records (Scotland) Act (PRSA) Update**

The IG Manager (Corporate Records), Ms Natali Higgins, provided an update on progress being made to implement the Records Management Plan (RMP) to improve the management of the organisation's corporate records.

Ms Higgins advised that following submission of the update to the PRSA Assessment Team, they had provided their final response on 11 August 2022. Overall feedback had been positive and the Assessment Team was satisfied with progress made and compliance with each element of the programme. Ms Higgins advised that while this positive feedback was welcomed, this was a high level overview

report and there was still significant work to be done to improve the management of corporate records across the organisation.

The Committee was advised that NHSAA's focus continued to be elements 4 and 11, Business Classification Scheme and Audit Trail, both of which had a dependency on the implementation of M365. The report outlined the preparatory work taking place. Additionally, the organisation required to ensure that there were measures in place to support element 15 (Public records created or held by third parties) which was introduced in 2019. At present there had been little progress in this area.

Ms Higgins provided an update on changes to Corporate Records Management staff resource following her secondment to the Scottish Government for three days per week. An Assistant Corporate Records Manager role had been developed and a recruitment process was ongoing. Ms Higgins would continue to strategically lead the work programme and provide direction to the Assistant Manager, who would be responsible for operational delivery aspects of the programme. Ms Higgins reassured in response to a question from a Committee member that she would continue to progress as much work as possible during her two days per week with NHSAA. It should be possible to pick this work up again quite quickly once the new Assistant Manager is in post.

Ms Higgins advised in response to a question from a Committee member that she was working with the Head of Planning and Information and the Health Records Manager in relation to element 15, which mainly related to health records. The PRSA Assessment Team had provided proposed contract clauses which were still under local review. Following approval, the team would contact third parties to discuss contracts/service level agreements in place.

The Head of IG and DPO, Ms Ann Wilson, confirmed that in addition to the detailed annual PRSA update, the Committee will receive a focused six monthly exception report to enable members to monitor progress against key actions outstanding. The IG Operational Delivery Group will routinely monitor progress against the Progress Update Review.

Outcome: Committee members discussed and were assured of the work being done to ensure compliance with PRSA.

6. For Assurance

6.1 Information Security Breach report

The Head of IG and DPO, Ms Ann Wilson, provided an update on information security breaches which had occurred within NHSAA in Quarter 1, April to June 2022.

Ms Wilson outlined the definition of a data breach under the UK

General Data Protection Regulation (UK GDPR). There were two tiers of breaches related to personal data and breach of principles. A breach may also require to be reported by Digital Services through Network and Information System (NIS) Regulations. Ms Wilson explained that it was possible for NHSAA to be fined three times for one incident and she underlined the need to ensure robust management of breaches.

Committee members were advised that there were 24 breaches during the reporting period, with 22 classed as personal data breaches. None of the 22 personal data breaches were considered to be notifiable to the Information Commissioner's Office (ICO). All remedial actions had been taken and lessons learned shared. A number of breaches were due to human error, such as sending an email to the wrong person, and work was ongoing to identify tools and quick fixes through Microsoft 365.

Ms Wilson advised that the number of breaches appeared low given the size of the organisation. Work would take place to encourage and support staff to report breaches so that any gaps could be identified, improved processes put in place and learning shared across the organisation. As this work progressed, it may result in an increase in the number of breaches being reported in future reports to the Committee. Committee members emphasised that it would be important to have an audit trail following communication and training for staff to correlate this activity with any increase in breach reporting.

Ms Wilson advised in response to a question from a Committee member that she would meet with the IG team later in the day to consider data breach reporting and what could be done to improve the process and ensure that data breaches are reported to the ICO within the required timescale.

Outcome: Committee members discussed and were assured of the work being done to promote compliance with Data Protection Legislation.

6.2 **Freedom of Information (FOI) report**

On behalf of the FOI Officer, the Head of IG and DPO, Ms Ann Wilson, presented the six monthly report on FOI activity.

The Committee was advised that 94.6 per cent of FOI requests received in the first half of 2022 were responded to within the statutory timescale, an increase from 91.5 per cent in the same period in 2021. A total of 350 requests were received, a 23% increase on the number of requests received in the same period in 2021.

Ms Wilson advised that many FOI requests were complex and required input from at least two Directorates. FOI Champions had an important role in supporting the FOI Officer to respond to requests.

Ms Wilson advised that there had been an increase in the number of

requests for internal reviews, as detailed in the report, with activity returning to pre-pandemic levels which would impact on the FOI team and Directorates as this workload increased.

On 12 April 2022 the Board had received notification of an appeal from the Scottish Information Commissioner (SIC). However the request under appeal had not been submitted through the FOI route. It had been agreed with the Validation Officer that this be treated as an internal review in the first instance. The case had not yet been allocated to an investigating officer by the SIC.

Ms Wilson provided clarification in response to a question form a Committee member that quarterly data was provided to the SIC detailing FOI activity and exemptions that had been applied. Ms Wilson would add a note to future reports on the definition of part-answered requests. Committee members requested that five quarter data be provided in future reports to enable the Committee to monitor trends. **AW/TP**

Outcome: Committee members discussed and were assured of the work being done to ensure compliance with the Freedom of Information (Scotland) Act.

7. Governance

7.1 Information Governance Operational Delivery Group

The Head of IG and DPO, Ms Ann Wilson, presented the approved minutes of the meeting held on 29 April and draft minutes of the meeting held on 29 July 2022.

Outcome: The Committee noted the minutes of the meetings held on 29 April and 29 July 2022.

8. Risk

8.1 Information Governance Committee Strategic Risk Register

The Assistant Director, Occupational Health, Safety and Risk Management, Mr Hugh Currie, provided an update on risk management arrangements and the updated IGC risk register. The report had been discussed in detail at the Risk and Resilience Scrutiny and Assurance Group meeting held on 22 July 2022.

Mr Currie reported that there were two high risks being treated, risk ID 557, compliance – information governance and risk ID 603, service/business interruption – cyber incident. Risk ID 557 was reviewed in July 2022 and the risk grading did not change. Appendix 2 of the report provided more detail behind these risks.

Mr Currie advised that a Board workshop had recently taken place to review the Board's risk appetite statement and this was being progressed with plans to present at the next Board meeting on

3 October 2022 for approval.

Committee members highlighted discussion at item 5.1 above on Digital and Cyber Security, progress made through the NIS audit and the wider cyber security risks currently facing public sector organisations, and queried if the rating of 2 for likelihood was appropriate. Mr Currie confirmed that he would pick this up with the Director Infrastructure and Support Services and Acting Assistant Director for Digital Services out-with the meeting and ask them to review the risk for presentation at the next Risk and Resilience Scrutiny and Assurance Group meeting. **HC**

Risk 557 states that the Information Governance Committee will now receive a compliance matrix detailing NHS A&A's compliance with data protection legislation and accountability requirements. This will be on a six monthly basis. The Committee Chair queried what this matrix looked like and when it would be available and Mr Currie advised he would clarify the position. **HC**

Outcome: Committee members noted the report and work being done to manage strategic risks which fall under the governance remit of the IGC.

8.2 **Risk issues to report to Risk and Resilience Scrutiny and Assurance Group (RARSAG)**

Committee members were advised that the organisational risk related to Cyber Security and whether the rating of 2 for likelihood was appropriate would be reviewed and presented by Mr Derek Gemmell at the next RARSAG meeting. There were no other risk issues to report to RARSAG.

9. Key issues to report to NHS Board

9.1 Committee members agreed that the following key issues be reported to the NHS Board meeting on 3 October 2022:

- Digital and Cyber Security - reporting and monitoring arrangements.
- Update on the work being done to ensure compliance with the Public Records (Scotland) Act
- Suite of regular update reports received, including Health Records activities under the remit of IGC; Information Security Breaches; Freedom of Information; and the IGC Strategic Risk Register report. The Committee also received minutes of IGODG meetings on 29 April and 29 July 2022. There were no major concerns arising from these reports.

10. Any Other Competent Business

10.1 **IGC Vice Chair Vacancy** – Committee members unanimously supported Ms Sheila Cowan’s nomination as IGC Vice Chair with immediate effect.

Approved by the Committee on 14 November 2022

11. Date and Time of Next Meeting
Monday 14 November 2022 at 10am, MS Teams

Signed by the Chair  Date: 14 November 2022